Overview of the Privacy Act

United States Army

Overview

After completing this training course, you should be knowledgeable on:

- The purpose of the Privacy Act and policy objectives
- Who is covered by the Privacy Act
- Restrictions on disclosing Privacy Act records
- Civil and criminal penalties
- Safeguarding Personally Identifiable Information (PII)

What is the Privacy Act?

The Privacy Act balances the government's need to maintain information about individuals with the right of individuals to be protected against unwarranted invasion of their privacy.
This:

- Regulates the collection, maintenance, use, and dissemination of **Personally Identifiable Information (PII)** by Federal Executive Branch Agencies
- Limits the unnecessary collection of information about individuals

What is PII?

Personally Identifiable Information (PII) is defined as: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, DOD ID, biometric records alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, and so forth. (OMB M-07-16)

Privacy Act Objectives

- To restrict **disclosure** of information and records maintained by agencies
- To grant individuals the right to seek **amendment** of agency records maintained on themselves
- To grant individuals increased rights of **access** to agency records maintained on themselves
- Establishes rules that govern the collection and use of personal data

Who is covered by the Privacy Act?

The Privacy Act applies to:

- Federal Agencies
- Living U.S. Citizens
- Legal aliens lawfully admitted for permanent residence

The Privacy Act regulates the way individuals' personal information is handled.

As an individual, the Privacy Act gives you greater control over the way that your personal information is handled.

What is covered by the Privacy Act?

The Privacy Act allows you to:

- know why your personal information is being collected, how it will be used, and who it will be disclosed to
- ask for access to your personal information (including your health information)
- ask for your personal information that is incorrect to be corrected
- make a complaint about an entity covered by the Privacy Act, if you consider that they have mishandled your personal information

Disclosing Personally Identifiable Information

No agency or person shall disclose any record that is contained in a **system of records** by any means of communication to any person, except pursuant to:

- a **written request** by the individual to whom the record pertains, or
- the **written consent** of the individual to whom the record pertains

Restrictions on disclosing Privacy Act Records

There are twelve (12) exceptions to “No disclosure to Third Parties Without Consent” rule.

Twelve Exceptions Allow Agencies to Disclose PII Without a Consent

1. To employees with a legitimate need-to-know

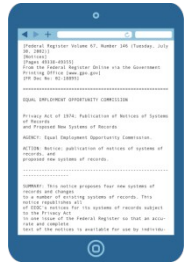
NEED TO KNOW

2. When the FOIA requires release

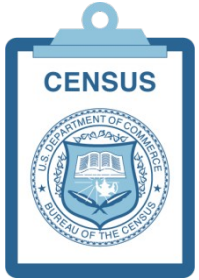
FOIA

Twelve Exceptions Allow Agencies to Disclose PII Without a Consent

3. For a “routine use” identified in the System of Records Notice (SORN) that has been published in the Federal Register

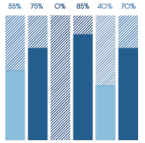


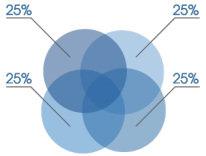
4. To the Census Bureau for purpose of conducting the census



Twelve Exceptions Allow Agencies to Disclose PII Without a Consent

5. For statistical research and reporting in which individuals will not be identified





6. To the National Archives and Records Administration

Twelve Exceptions Allow Agencies to Disclose PII Without a Consent

7. To civil or criminal law enforcement under U.S. control

8. For circumstances affecting the health or safety of the individual

Twelve Exceptions Allow Agencies to Disclose PII Without a Consent

9. To either House of Congress

10. To the Comptroller General

Twelve Exceptions Allow Agencies to Disclose PII Without a Consent

11. Pursuant to a court order (a subpoena signed by a judge)

12. To a consumer reporting agency in accordance with the Debt Collection Act

Information Sharing Concerns

Having a specific **need-to-know** means that access to the information in question is absolutely required to perform one's official duties

- **Need-to-know** may be established for official business, statutory law, and information sharing
  - For example: A person working in a finance division does not have a need-to-know about another person's medical information

Information Sharing Concerns

If a **need-to-know** has not been or cannot be established, the following actions should be taken:

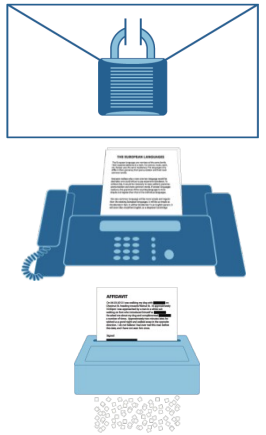
- Do **not** share the information in question

- If information has already been inappropriately released, **notify your manager** immediately; this is a **PII breach**

Information Sharing Concerns

To avoid the most common types of breaches, utilize the following best practices:

- Use a Privacy Cover Sheet as a cover when handling PII
- Always encrypt emails containing PII
- Avoid sending faxes containing PII when possible
- Dispose of documents containing PII properly



Civil and Criminal Penalties

Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect on the subject of the record may have different consequences:

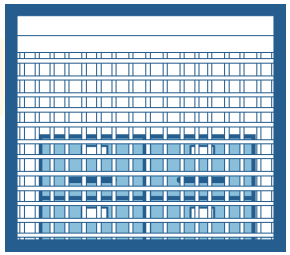
- **Civil penalties**: (Applying to the Agency)
  - The cost of actual damages suffered ($1,000 minimum)
  - Costs and reasonable attorney’s fees

Civil and Criminal Penalties

Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect on the subject of the record may have different consequences:

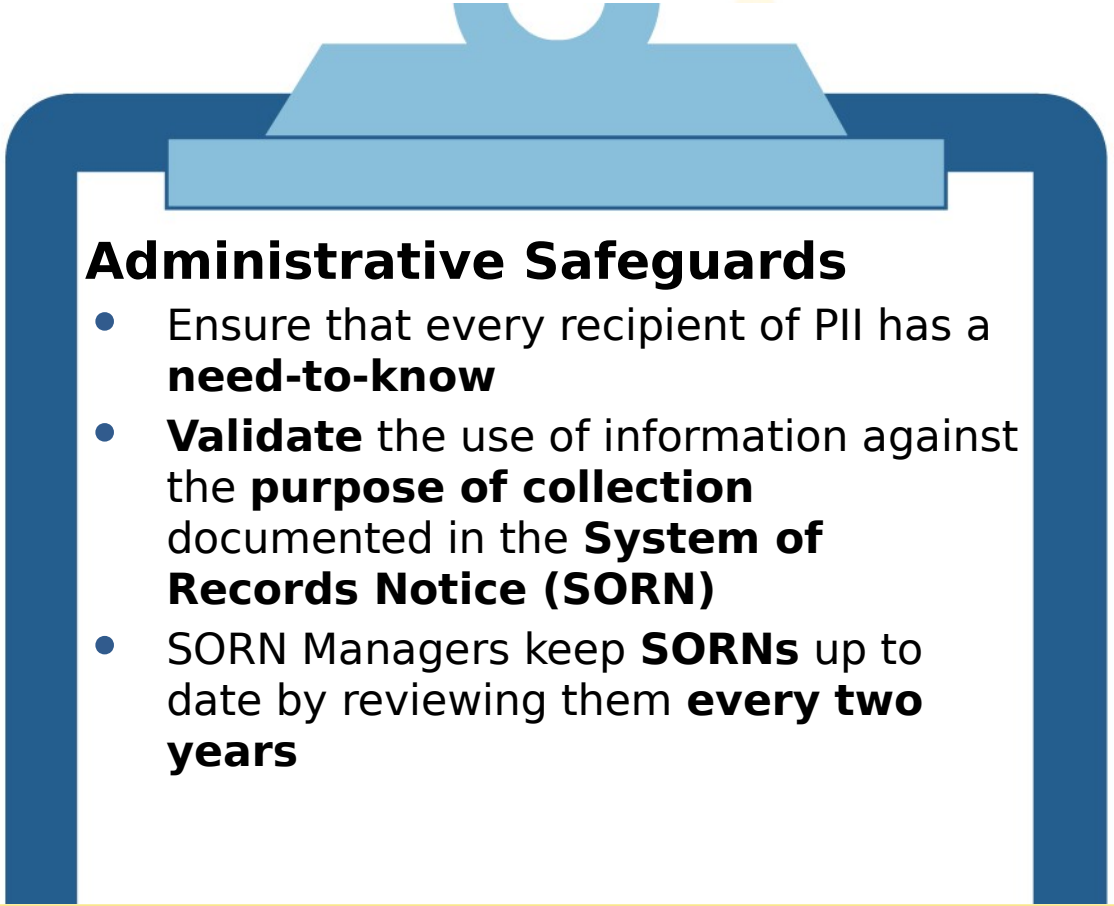
- **Accidental** infringement will result in discretionary discipline depending on the severity of the offense
- The "**willful violation**" of any Privacy Act provisions will result in **Criminal Penalties** including:
  - A misdemeanor charge
  - A maximum fine of $5,000

Safeguarding Personally Identifiable Information



- **Administrative** - Procedures implemented at the administrative level to protect private information.
- **Technical** - Technology-based instruments and procedures used to protect private information.
- **Physical** - The physical protections implemented for protecting private information

Safeguarding Personally Identifiable Information



Administrative Safeguards

- Ensure that every recipient of PII has a **need-to-know**
- **Validate** the use of information against the **purpose of collection** documented in the **System of Records Notice (SORN)**
- SORN Managers keep **SORNs** up to date by reviewing them **every two years**

Safeguarding Personally Identifiable Information

Administrative Safeguards

- Ensure telephone conversations are **private**
- Consult your **Component Privacy Officer** before collecting **PII**
- Include a **Privacy Act Data Cover Sheet** with all copies of documents containing **PII**
- Collect, use, maintain, and disseminate data that is **accurate, complete, relevant, and timely**

Safeguarding Personally Identifiable Information

Technical Safeguards

- **Encrypt all emails** that contain **PII**
- Use only **DoD-approved software** on your computer
- Do **not** use **flash (thumb) drives** for transporting **PII**
- **Never** use **personal equipment** to store **PII**
- Ensure that information is from a **government authorized source**

Safeguarding Personally Identifiable Information

Physical Safeguards

- Use **locks** to secure **PII** when stored
- **Dispose** of records according to established schedules in the SORN or procedures established by The National Archives and Records Administration
- **System Managers** should maintain a record of the movement of hardware and electronic media in their control, including to whom the equipment was issued, the date of issuance, and the date of return
- Implement policies and procedures to safeguard the **facility** and the **equipment therein** from **unauthorized physical access, tampering, and theft**

References

- Defense Privacy and Civil Liberties Office – http://dpclo.defense.gov
- DoD Directive 5400.11, “DoD Privacy Program,”
- DoD Regulation 5400.11-R, “Department of Defense Privacy Program,”
- DA&M Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,”